Testimony Of

Drew Bagley
Vice President & Counsel for Privacy and Cyber Policy
CrowdStrike

Before

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell, members of the subcommittee, thank you for the opportunity to testify today. We are at a pivotal moment in the cybersecurity challenges posed to our country. Today, nation states, criminal enterprises, and hacktivist groups alike can leverage sophisticated means to exploit unsophisticated vulnerabilities to conduct espionage, breach privacy, and wreak havoc on critical infrastructure, government systems, and businesses throughout the country. We are at a point where the stakes of defensive stagnation pose increasing risks in the face of threat actors' innovation. This is why it's so important to continually evolve in how we prevent, detect, and respond to cyber attacks.

Throughout my career, I have seen firsthand the challenges and opportunities of improving American cybersecurity from my work in the private sector, government, and academia. For nearly a decade, at CrowdStrike, a leading cybersecurity company, I have had a front row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the US and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program. I have been asked to speak here today from a stakeholder perspective. Accordingly, my testimony is informed not only from my experience but also by my continued engagement with government agencies through formal and informal advisory roles, including as a member of CISA's Joint Cyber Defense Collaborative (JCDC).

At CrowdStrike, we have a unique vantage point on cybersecurity threats and the innovation necessary to stop them. We not only protect 15 of the largest 20 banks in the US but also provide our cybersecurity technology and services to thousands of small and medium sized businesses. This means that it is not only possible for small organizations to leverage the same cybersecurity technologies as complex multinational enterprises but that it is becoming more common.

Increasingly, fundamental aspects of cybersecurity program design are applicable everywhere–including for the ongoing transformation in U.S. federal cybersecurity.

CrowdStrike works with CISA in a variety of ways across key programs and activities. We were one of the original plank holders of JCDC and remain active members to this day. We provide cyber threat intelligence and cybersecurity technology offerings to CISA that help it defend not only its own networks but those of some other government departments and agencies as well. Lastly, we are a consumer of CISA's advisories and a key technology provider for its other stakeholder groups, like critical infrastructure entities.

Key Developments

This hearing is timely for three key reasons. First, over the past couple of years CISA has reached its stride across a number of operational and planning functions (described in more detail below). Second, major transitions are taking place in federal cybersecurity overall, with an emphasis on security program modernization and Zero Trust Architecture. CISA is a key actor and implementer in these areas. Third, geopolitical conditions have yielded a worsening cyber threat environment overall. Russia's war in Ukraine and heightened competition with China are just two of several active examples where risks are mounting.[1]

Now is an impactful time to review the state of cybersecurity overall and evaluate CISA's considerable progress and contributions.[2] As DHS and CISA leadership and Members of this Committee prepare jointly to realize the vision of *CISA 2025,*[3] we can identify fruitful areas for continued development, alignment, and investment, where appropriate.

The State of Cybersecurity

Cybersecurity outcomes vary substantially across different sectors. Different sectors face different threats, have different constraints and capacities, and have different tolerances to risk or disruptions. To this end, I'd like to survey the state of cybersecurity across a few key CISA partner segments.

Federal Civilian Executive Branch (FCEB). Going back 20 years, Federal government agencies often had considerable cybersecurity strengths relative to their private sector counterparts. However, as time went on and cyber attacks increasingly occurred without the use of malware, parts of the private sector met and exceeded FCEB cybersecurity performance by adjusting to new realities. In some instances, government IT standards and controls failed to evolve at the rapid pace of innovation within the commercial IT and cybersecurity space. Large Federal Cybersecurity

---

[1] *See Adam Meyers, Testimony on Securing Critical Infrastructure Against Russian Cyber Threats,* House Homeland Security Committee (March 30, 2022) (How Russia-nexus adversaries use cyberattacks and recommendations for U.S. readiness), https://docs.house.gov/meetings/HM/HM00/20220405/114553/HHRG-117-HM00-Wstate-MeyersA-20220405.pdf.
[2] *See CISA Strategic Plan 2023-2025*, CISA (September 2022), https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.
[3] *See CISA 2025 Overview,* Committee on Homeland Security, House of Representatives (October 13, 2022), https://homeland.house.gov/cisa-2025/.

programs (e.g., National Cybersecurity Protection System (NCPS) or EINSTEIN, and the Continuous Diagnostics and Mitigation Program (CDM)) set ambitious goals aimed to standardize and scale approaches to government cybersecurity, but even with considerable investment over the years, that aim remains unmet.

Over the past several years, however, the Federal cybersecurity community has made some significant strides. Recent developments are trending positively with the embrace of key cybersecurity concepts like centralized visibility of IT infrastructure to detect and respond to incidents. Significantly, E.O. 14028 on *Improving the Nation's Cybersecurity*[4] mandated the use across the FCEB of key best practices, like enhanced logging, as well as now-baseline technical solutions like Endpoint Detection and Response (EDR). The release of the Office of Management and Budget's *Federal Zero Trust Strategy*[5] in January 2022 was another key decision enforcing the use of sound approaches, like increased adoption of cloud-based technologies, credential management practices,[6] and defensible IT architectures. Even as implementation continues, these initial efforts are yielding positive results.

CISA plays an essential role in strengthening FCEB cybersecurity. As recently as a couple of years ago, CISA had just a few programs (e.g., NCPS, CDM, Trusted Internet Connections (TIC)) and a few authorities (e.g., Emergency Directives, Binding Operational Directives[7]) to meet this mandate. But the Solarium Commission's recommendation as enacted by Congress to formally elevate CISA to become the operational CISO of the FCEB, including by providing government-wide, proactive cyber threat hunting capabilities, considerably strengthened CISA's toolkit. Further, actions taken by CISA to implement E.O. 14028, particularly with regard to the EDR program, are helping to realize this vision.

The stakes are high. The FCEB continues to be a key target of threat actors that seek to do harm to the United States. Friends and allies continue to look to the U.S. Government as a model for how to organize their own government cybersecurity efforts. And importantly, the government must lead by example on cybersecurity. CISA's efforts to strengthen security across the other entities (e.g., critical infrastructure or state and local governments) will lack credibility if the FCEB is poorly secured.

Large Enterprises. On balance, the most sophisticated large enterprises in the U.S. have seen stronger cybersecurity outcomes in recent years, even as threats evolve and multiply. Over the past year, we've observed an increase in vulnerability reuse and increased reliance on access brokers to facilitate initial infiltration into target organizations. We've also witnessed increased targeting of–and mounting costs from–breaches of legacy infrastructure.[8] Supply chain attacks, which can be

---

[4] *See Executive Order on Improving the Nation's Cybersecurity,* The White House (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] *See M-22-09 Memorandum for the Heads of Executive Departments and Agencies,* Executive Office of the President, Office of Management and Budget (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[6] *See 7 TYPES OF IDENTITY-BASED ATTACKS,* CrowdStrike (January 10, 2023), https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-based-attacks/.

[7] *See Cybersecurity Directives,* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/directives.

[8] *See 2023 Global Threat Report,* CrowdStrike (2023). https://www.crowdstrike.com/global-threat-report/.

targeted but also used to breach many dependent organizations in a single campaign, remain a key concern.

Some large commercial enterprises have greater flexibility and stronger security budgets than other entities, and thus serve as an important proving ground for new technologies, practices, and architectures. From this, recent innovations like Zero Trust and cloud-native EDR have become today's cybersecurity essentials. In the near future, we should expect more attention from other sectors on emerging enterprise security concepts like Extended Detection and Response (XDR), identity threat protection,[9] as well as continued adoption of managed security services (discussed in more detail below).

Small- and Medium-sized Businesses (SMB). These entities include everything from the family-owned corner store in each of our communities to startups creating new technologies that could change the world. These companies operate off of very different templates but nevertheless share two key features. First, resources are scarce. Second, a multi-day business disruption might well destroy the company. Resource scarcity means there's no place for complex cyber defenses, and few if any 'spare cycles' for participation in demanding or time-consuming information sharing initiatives. Sensitivity to disruption means these organizations are particularly vulnerable to ransomware and "lock-and-leak" attacks.

Among the most positive developments in this space in recent years is the growing affordability and accessibility of managed security services, as well as managed threat hunting services. Organizations increasingly look to professional providers to manage the overwhelming majority of defense actions–under tight service level agreements–24 hours a day, 7 days a week, 365 days a year.

State, Local, Tribal, and Territorial (SLTT) Entities. Over the past few years, SLTT entities have faced a withering threat environment, most notably from criminal ransomware actors. Materially all SLTT entities face budgetary and personnel constraints, and rely upon critical legacy applications and IT infrastructure. Nevertheless, over that same time horizon, cybersecurity outcomes within the sector have diverged significantly. As Members of this Committee know well, many SLTT organizations faced severe incidents and events, and in some instances citizens suffered disruption of key services.

Counterintuitively perhaps, over this timeframe the most forward-leaning states and cities were meaningfully further ahead than most of the FCEB in centralizing and modernizing defenses. This was generally achieved through a key service provider–typically a Department of Technology–implementing and managing transformative technologies like EDR and other important security concepts and practices. In addition to leveraging a centralized provider, these states often had no inflexible security program that acted as a barrier to experimentation and technology

[9] *See Andrew Harris, CrowdStrike Falcon Identity Threat Protection Added to GovCloud-1 to Help Meet Government Mandates for Identity Security and Zero Trust*, CrowdStrike (June 1, 2022), https://www.crowdstrike.com/blog/how-falcon-identity-threat-protection-helps-meet-identity-security-government-mandates/.

adoption. In addition, community-oriented support efforts, such as those led by the Center for Internet Security, have been a key part of stronger defenses.

The State and Local Cybersecurity Improvement Act, which passed into law in the Infrastructure Investment and Jobs Act of 2021 was a positive step in ensuring state and local governments have the funding needed to centralize and modernize cyber defenses. We appreciate former subcommittee Chairwoman Clarke, Chairman Garbarino, and other members of the committee for their leadership on this important issue.

Critical Infrastructure. Most critical infrastructure owners and operators face the same set of hardships outlined above: severe threat environment, personnel and budget constraints, and legacy applications and IT infrastructure. But they have the added challenges of complex Operational Technology (OT) that in some instances is obsolete and/or esoteric. In addition to these conditions there is increased interest from policymakers in regulatory measures designed to enhance cybersecurity.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, which strengthens reporting obligations for critical infrastructure players, is the most meaningful step to date.[10] CIRCIA's authors–notably Members and key staff on this Committee–recognized these risks and included two key provisions. The first is a Cyber Incident Reporting Harmonization Council that should reconcile duplicative or conflicting regulations. The second is a generous timeline for CISA to articulate particulars (like thresholds) in a clear and straightforward manner. CISA has solicited stakeholder feedback to those ends, to which we, and many others in the community, were happy to contribute ideas and suggestions.[11]

International. Although somewhat beyond the scope of this hearing, we should take a moment to reflect on international cybersecurity. U.S. allies' public sector organizations, laws, and policy debates tend to reflect somewhat developments here in Washington. This is an incredible leadership opportunity. Efforts like the International Counter Ransomware Initiative[12] serve as a good example for how to use this influence to strengthen the cybersecurity ecosystem globally. Across relevant areas of law and policy, we should embrace interoperable approaches that simplify collaboration between governments, NGOs, and industry players. In addition, the U.S. should be receptive to areas where other countries have identified helpful policies. These include, for example, policies that support the startup ecosystem, and national privacy laws that simplify data protection and the cross-border data flows integral for modern cybersecurity.[13]

---

[10] *See Public Law 117 - 103, Division Y, Cyber Incident Reporting for Critical Infrastructure Act - Consolidated Appropriations Act, 117th Congress (March 15,* 2022). https://www.congress.gov/bill/117th-congress/house-bill/2471/text.
[11] *See CrowdStrike Response to RFI on Cyber Incident Reporting for Critical Infrastructure Act (November 14, 2022),* https://www.crowdstrike.com/wp-content/uploads/2023/02/RFI-Incident-Reporting-for-Critical-Infrastructure-Act-of-2022.pdf.
[12] *See International Counter Ransomware Initiative 2022 Joint Statement,* The White House (November 1, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.
[13] *See Drew Bagley, Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance,* CrowdStrike (January 27, 2023), https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance.

Public-Private Collaboration

The Joint Cyber Defense Collaborative (JCDC). Information sharing in the cybersecurity space is a complex topic and longstanding policy priority. For two decades, various information sharing efforts–narrow and broad; informal, quasi-official, and official; *ad hoc* and enduring–have arisen from a desire within the cybersecurity community to do more. While the Cybersecurity Act of 2015 sought to address this problem head on,[14] structural impediments to comprehensive sharing and collaboration remain.[15] And as a practical matter, we are unlikely to identify a "silver bullet" solution to a problem with this many complexities. However, the formation of JCDC in August 2021 was a key development in promoting sharing and collaboration. In the time since, JCDC has created a platform for key players in industry and government to voluntarily work toward common goals.

While we would generally defer to CISA Leadership to describe key outcomes, we can say that CrowdStrike values the partnership opportunity. We continue to invest time and expertise in the JCDC community, and we look forward to continued, shared efforts to promote better cybersecurity.

As JCDC matures, we believe the effort can continue to improve. Two suggestions:

- **Consider approaches that stratify or segment membership to maintain trust**. As the group expands, JCDC leadership should account for the possibility that some members may become less willing to share details about sensitive issues. JCDC has addressed this concern by maintaining clear direct channels of communication with participants, and creating ad hoc working groups with a subset of members. These are important measures, but additional subgroup governance may help promote more active and applied sharing. Articulating long-term aims for membership composition may also be of value.
- **Strengthen *administrative* Customer Relationship Management (CRM) practices**. This would ensure consistent notification of participant stakeholders about upcoming opportunities, events, engagements, etc. A designated partner "JCDC relationship owner" should be able to flexibly add or remove corporate participants from various JCDC workstreams to facilitate participation from particular personas (e.g, according to function, experience, protocol, etc.).

To their credit, JCDC leadership and staff have been proactive about seeking feedback from participants. We have provided suggestions along these lines to them directly and believe it is taken seriously. Like any "startup," we anticipate continued iteration as the group matures into its full potential.

Ecosystem. CISA contributes to the cybersecurity ecosystem in a variety of other ways. Support to key partners in the SLTT community; advice and tools for enhancing infrastructure, Industrial

[14] *See Public Law 113-113, Division N, Cybersecurity Act of 2015.* 114th Congress (December 18, 2015), https://www.congress.gov/bill/114th-congress/house-bill/2029/text

[15] *See George Kurtz, Questions for the Record - Hearing on the Hack of U.S. Networks by a Foreign Adversary,* Senate Select Committee on Intelligence (February 23, 2021) (How the private sector has promoted practical information sharing),https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf.

Control Systems (ICS), and OT security; alerts and notifications for IT security, particularly around emerging vulnerabilities; and leadership on workforce topics all contribute to better cybersecurity outcomes. Each of these issue areas is complex and requires specific expertise. CISA's contributions in this realm continue to mature and become more valuable over time.

There remains a gap in cybersecurity performance between the "haves" and the "have-nots," which threat actors continue to exploit and which CISA cannot solve alone. To this end, we are pleased to see reference in the new National Cybersecurity Strategy to shifting the burden for cybersecurity to those best positioned to mitigate risks. This includes, where appropriate, holding platform providers accountable for the security of their products.[16] As a community, we should no longer tolerate certain software vendors externalizing the costs of–or worse, nakedly monetizing–insecure software applications.[17] While this policy concept must be made more concrete, a reasonable first step is ensuring that we're not rewarding vendors that cause harm. To this end, the government can lead by example by using its own procurement power to shape market dynamics. This is clearly a productive area for continued congressional oversight.

Recommendations

1. **The entire field must become more responsive in adapting to lessons learned**. Unfortunately, cyberattacks with the potential for systemic implications take place with increasing regularity. However, organizations are uneven in adopting key lessons, from new security controls and mitigations to more secure architectures. From our vantage point, key lessons of recent breaches include:

- Use managed security services where practical to augment internal security staff and attain responsive and comprehensive security coverage.
- Adopt cloud-based IT systems and where possible, leverage cloud-based security tools to achieve scalability and speed.
- Employ Zero Trust Architecture, with emphasis on identity threat protection, to defend an increasingly diffuse IT infrastructure and radically reduce lateral movement during breach attempts, bringing us closer to cyber and mission resiliency.

2. **We must approach regulation deliberately and harmonize to the greatest extent possible.** Even as CIRCIA advances through rulemaking, independent regulators are pursuing new obligations[18] and the National Cybersecurity Strategy foreshadows additional actions at the sector-level.[19] Each of these measures is well-intended, but taking place simultaneously and with different stakeholders. At best, they will close longstanding gaps and strengthen national resilience.

---

[16] *See National Cybersecurity Strategy, page 20.* The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[17] For one example of a persistent security issue, see *George Kurtz, Testimony on Cybersecurity and Supply Chain Threats,* Senate Select Committee on Intelligence (February 23, 2021) (Extended discussion on emerging cybersecurity controls and practices), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf. p. 5.

[18] *See TSA issues new cybersecurity requirements for airport and aircraft operators,* Transportation Security Administration (March 7, 2023), https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

[19] Even prior to CIRCIA and recent efforts, data breach victims commonly faced more than 50 different reporting requirements in the U.S. alone, with additional international obligations in many cases.

At worst, they risk yielding burdensome, distracting, and costly compliance obligations without additional security gains. Optimizing for the former is among the most important challenges the cybersecurity policy community faces at this time. Our hope is that continued collaboration between potential regulators and/or muscular harmonization efforts will help avert worse outcomes. The best advice we can offer is:

- Be deliberate about advancing new requirements;
- Provide formal commenting periods for stakeholders to contribute views;
- Use principles-based requirements rather than burdensome and inflexible compliance-based approaches;
- Include provisions to regularly review and if necessary modify, update, or deprecate requirements or controls based on developments in the threat environment or technology ecosystem;
- The DHS Cyber Incident Reporting Council established under CIRCIA should operate with vigor, and work to clearly identify and reduce duplicative reporting; and
- Set the goal of all federal agencies showcasing cybersecurity best practices with a particular emphasis on those that regulate cybersecurity "walking the walk."

3. **As a community, we should focus more attention on national incident response capacity.** JCDC should continue coordinating and developing community response plans and CISA should weigh potential JCDC contributions for the purposes of forthcoming revisions to the National Cyber Incident Response Plan (NCIRP).[20] If the Russian threat actors responsible for the major supply chain attack or the Chinese threat actors responsible for the Microsoft Exchange hacking campaign in 2021 had deployed ransomware or pseudo-ransomware at scale, large segments of the American economy would have been paralyzed. A CISA-administered program to retain outside providers for emergency incident response to attacks at entities of systemic importance could be of tremendous value in a future contingency.[21] This could mitigate crippling impacts and ensure CISA had the ability to orchestrate response activities and maintain insight into findings in real time.

4. **We must empower defenders with cutting edge cyber-defense capabilities.** Defenders with leading solutions are energized with radically improved morale. Too often, defenders are hobbled with inefficient and ineffective technologies. When these inevitably fail, they begin to feel like little more than a punching bag for adversaries, and that their best efforts are for naught. But when people are empowered, they can see their impact each day and can remain focused on the importance of their mission. To the extent that this Committee can promote access to better tools, that will absolutely strengthen cybersecurity outcomes. For the FCEB, this means the full adoption of technologies mandated in E.O. 14028 like EDR and, ultimately, better access to managed security services to augment staff. To highlight another opportunity, we believe it's time to have a more

[20] *See National Cybersecurity Strategy, page 12.* The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[21] *See Robert Sheldon,Testimony on Protecting American Innovation, Senate Select Committee on Intelligence (September 21, 2022),* https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

serious conversation as a community about using tax mechanisms to speed adoption of key technologies in the SMB space.[22]

5. **The community must attract and retain top cybersecurity talent.** The level of talent in our field–across industry and government–is deeply inspiring. Based on our experience, the central motivator for people in the field is a sense of mission. A key challenge we have as a community is overburdened staff leading to burnout, a concern that underpins some of my previous comments on leveraging managed services and mitigating time-consuming and ineffective compliance obligations. Further, aligning roles to each organization's key missions–and in the case of government authorities–helps people recognize the uniqueness of their contributions. A second challenge is expanding recruitment efforts to grow additional talent. To this end, I was pleased to announce during my participation at a White House Summit last month that CrowdStrike would soon launch an emerging leaders program focused on diverse candidates.[23] We must continue efforts to fuel the cybersecurity talent pipeline.

CISA's evolution is the culmination of non-partisan efforts under four consecutive presidential administrations, and CISA has received numerous new key authorities and increases in funding over the past several years. Ultimately, in each passing year it is important to ask whether the US government is better able to prevent, detect and respond to cyber attacks. Accordingly, I am pleased to see this committee has identified key oversight areas in the CISA 2025 initiative to put CISA on track to fully implement those authorities and fulfill the mission Congress has entrusted it with. CrowdStrike looks forward to continuing and building upon its trusted relationship with CISA, and playing our part in empowering it to effectively carry out its mission.

Thank you for the opportunity to appear in front of you today, and I look forward to your questions.

###

[22] *See Robert Sheldon, Testimony on Protecting American Innovation,* Senate Select Committee on Intelligence (September 21, 2022), https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

[23] *See Readout: Office of National Cyber Director Hosts Roundtable on "The State of Cybersecurity in the Black Community"* The White House Briefing Room (February 28, 2023), https://www.whitehouse.gov/oncd/briefing-room/2023/02/28/readout-office-of-national-cyber-director-hosts-roundtable-onthe-state-of-cybersecurity-in-the-black-community/.

Testimony of Heather Hogsett

Senior Vice President, Technology and Risk Strategy for BITS, the Technology Policy Division of the Bank Policy Institute

Before the U.S. House Subcommittee on Cybersecurity and Infrastructure Protection
"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell and Honorable Members of the Subcommittee, thank you for inviting me to testify. I am Heather Hogsett, Senior Vice President of Technology and Risk Strategy for BITS, the technology policy division of the Bank Policy Institute (BPI).

BPI is a nonpartisan policy, research and advocacy organization representing the nation's leading banks. BPI members include universal banks, regional banks and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies and market utilities on cyber risk management and critical infrastructure protection, fraud reduction, regulation and innovation.

I also serve as Co-Chair of the Financial Services Sector Coordinating Council (FSSCC) Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency (CISA), as well as financial regulatory agencies.

Financial Institutions and Cybersecurity

Banks and other financial institutions are increasingly under cyber-attack by foreign nations and criminal groups seeking to disrupt the financial system and undermine the functioning of the U.S. economy. The financial sector takes these risks seriously and has a long history of working across industry and with government partners to address and manage these risks.

As one of 16 critical infrastructure sectors, the financial industry formed and actively participates in the FSSCC[1] and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] — both of which have served as leading examples other critical infrastructure sectors have sought to replicate. We also lead cybersecurity and operational resilience collaboration through public-private partnerships with our Sector Risk Management Agency (SRMA) — the U.S. Department of the Treasury — the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and importantly with our regulators.

A major part of these industry efforts is focused on in-depth information sharing to accelerate and amplify public-private cooperation. During the nearly two decades of work, we have established exercise programs through the FSSCC and FS-ISAC that have covered a wide range of possible events such as destructive malware, an outage at a large service provider, or a pandemic and addressed

[1] https://fsscc.org/
[2] https://www.fsisac.com/

managing public confidence during a crisis. More than 40 such exercises have been held to date and have included participants from across the industry, third parties, regulators, the U.S. Treasury Department, DHS/CISA and law enforcement agencies.

In addition to Treasury and CISA, we also work closely with financial regulators to address cybersecurity, third-party and supply chain risks and promote operational resilience across the sector. This work occurs with individual firms, through trade associations such as BPI, and via joint efforts between the FSSCC and its government counterpart the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by Treasury and includes 17 federal and state regulators.[3]

Experiences with CISA

Since its establishment in 2018 as an operational component of DHS, CISA has taken on an increasingly important role protecting federal civilian agencies and supporting security and resilience across critical infrastructure sectors. Following the important coordination role CISA filled during the COVID-19 pandemic to keep critical infrastructure working for America, there have been notable improvements in faster declassification and sharing of threat information, including a significant increase in publications, alerts and joint advisories with other government agencies such as the FBI and National Security Agency (NSA). These publications have become more frequent, timely and relevant and included recommended mitigation measures to help critical infrastructure entities better protect themselves, particularly midsize and smaller entities where the assistance is needed most. For example, CISA's recommended mitigations and tool kits to help entities protect themselves during the response to Solar Winds, Log4j and the ransomware attack against Colonial Pipeline were welcome for their timeliness and actionable nature. By creating a centralized repository for this information CISA has also made it easier for companies to quickly find and access relevant information and resources.

Its efforts to help raise awareness and promote baseline cybersecurity practices across all critical infrastructure sectors have been a welcome focus that will help reduce risk and improve national resilience. CISA also deserves credit for fostering collaboration and coordination across government entities including the banking industry and other critical infrastructure. Its work to date has built the foundation for trusted relationships and very importantly created resources to support those sectors that are resource constrained and in the earlier stages of building their cyber risk management programs.

The preparation and response to the Russian invasion of Ukraine highlight a number of these accomplishments. As tensions rose and the U.S. prepared for Russian aggression and the potential for retaliatory attacks, CISA's senior leadership, along with senior leaders at Treasury, DHS and the FBI, was in regular communications with financial institutions and organizations like the FSSCC, FS-ISAC and the Analysis and Resilience Center for Systemic Risk (ARC). CISA created the "Shields Up" campaign to raise awareness and urge critical infrastructure companies to shore up their defenses and actively share suspicious information with the government to provide an early warning of attacks. During this time, CISA created a new bi-directional communication mechanism to provide for near real-time information sharing among trusted partners in both industry and government that had never previously been done. This coordination role was invaluable for our industry and others and provided a streamlined mechanism to exchange threat information and share timely updates to those operating some of the nation's most critical infrastructure.

[3] www.fbiic.gov

Evolving for the Future

Looking ahead, it will be important for CISA to establish a clear path for maturing and scaling its operations, including ensuring these programs and initiatives have stakeholder input and will continue despite future changes in leadership. A number of the efforts to date have been in response to current cyber threats, which was and continues to be important, but CISA is also uniquely positioned to address longer-term strategic planning and cross-sector risk mitigation that will be particularly valuable for mature sectors. As CISA continues to evolve, we encourage a focus on the following areas:

- ***Cyber Incident Reporting and Harmonization – Supporting Response and Recovery***
  Last year, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, requiring critical infrastructure companies to report ransomware payments and cyber incidents to CISA. BPI supported this legislation which we believe will help improve national cyber defense by providing CISA and other government agencies with timely and relevant information to assess and analyze cyber threats across sectors, improve the alerts and security services CISA provides and ultimately provide earlier warning of potential attacks so companies can better defend themselves. Under the law, CISA must conduct a rulemaking process, seek input from stakeholders, and develop the necessary systems and processes to collect, analyze and share reported information while ensuring strong data security and protection measures are in place.

  As CISA crafts rules under CIRCIA, it is also required to harmonize the new requirements with existing regulatory reporting to avoid conflicting, duplicative or burdensome requirements. Given the comprehensive set of cybersecurity and incident notification rules[4] that financial institutions already comply with, harmonizing and aligning the new rules will be important to ensure cyber defenders can maintain focus on protecting the firm rather than complying with multiple government reporting requirements.

  This is a significant undertaking that CISA must get right from the outset and will require extensive coordination with critical infrastructure entities, SRMAs, other government agencies and independent regulators. As a critical infrastructure sector that has had mandatory cyber reporting requirements for more than 20 years and has invested significant time and resources into harmonizing and driving toward regulatory convergence, this is a key area of focus. CISA should ensure that definitions, timelines, thresholds and required incident information are aligned with existing requirements and designed to avoid interfering with response and mitigation at an affected firm.

  BPI recommends that CISA build a streamlined reporting system that accomplishes the following: 1) allows an impacted firm to report incident information once and have it shared, as appropriate, with SRMAs, regulators and law enforcement agencies; 2) provides CISA with timely and relevant information useful to assessing trends, improving analysis, and the development of alerts, tools and services that can be provided to critical infrastructure companies; and 3) maintains its role as a trusted channel for information and communications, preserving privacy and confidentiality while supporting the response and recovery of an impacted entity.

[4] https://staging4.bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/

- ***Identification and Prioritization of National Systemic Risks***
  Identifying critical infrastructure assets that are most important to our national security would help prioritize resources and guide public-private collaboration to prevent or mitigate threats and prepare for potential response and recovery needs.

  Financial institutions have existing designations such as the Systemically Important Financial Institution designation that stems from the Dodd-Frank Act of 2010 and requires firms to adopt enhanced measures for security and resilience and includes additional oversight and examination by financial regulators. Many of these firms are also included in the Section 9 process, established by Executive Order 13636 in 2013 and managed by DHS, which recognizes firms where a cyber incident could result in "catastrophic regional or national effects on public health or safety, economic security or national security."

  Similarly, in 2019, CISA created a list of 55 National Critical Functions that are functions "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[5] CISA is in the process of working with SRMAs to decompose or analyze these further. At the same time, CISA is developing a new designation for Systemically Important Entities (SIEs) and was appropriated an increase of $1.9 million for the creation of an SIE Program Office.

  Financial institutions are very supportive of efforts to better identify and prioritize cross-sector risks; however, the current approach appears disjointed and opaque, making it challenging for industry to provide input or information that might be helpful. Past proposals to create an SIE or Systemically Important Critical Infrastructure (SICI) designation would have duplicated existing designations and requirements on financial institutions, diverting resources from defending against threats to regulatory compliance.

  As CISA continues this work, we encourage greater transparency and clarity in the approach, what it intends to accomplish, and how an SIE designation fits with related areas of work such as the Section 9 list, NCFs and sector-specific systemic risk designations such as SIFI. CISA should not only avoid duplication or overlap with other systemic designations and their requirements but also leverage work that has already been done in the more mature critical infrastructure sectors. Financial institutions have worked through the ARC to analyze financial sector systemic risks and are ready to work with CISA to develop a framework for assessing risks and critical dependencies across sectors.

- ***Fostering Cross-Sector Coordination and Operational Collaboration***
  CISA's role as national coordinator for critical infrastructure security puts it in a unique position to support collaboration among more mature sectors and the government to reduce risk and disrupt threats. Since 2017, the financial, energy and communications sectors have conducted joint planning and exercises to address cyber threats that could impact or cascade across the three sectors. CISA supported the creation of the "tri-sector" working group which is a good example of fostering and enabling collaborative efforts.

[5] https://www.cisa.gov/national-critical-functions

CISA's Joint Cyber Defense Collaborative (JCDC) was helpful in bringing together industry and government partners to improve visibility and communication in response to geopolitical tensions and the Russian invasion of Ukraine. This response-oriented focus, however, has not fulfilled the need for longer-term strategic planning across government agencies and the private sector. As originally authorized by Congress,[6] CISA was charged with creating a Joint Cyber Planning Office (JCPO) to develop plans for cyber defense operations and coordinated actions that public and private sector entities could take to protect, mitigate, or defend against malicious cyber-attacks. To date, we have not seen the JCDC engage in the type of planning directed by Congress but continue to believe this would be beneficial for financial institutions and other more mature sectors.

The recently released National Cybersecurity Strategy recognizes that the private sector has growing visibility into adversary activity and calls for enhancing public-private operational collaboration to disrupt adversaries.[7] Through our relationship with Treasury as our SRMA, we have robust partnership and dialogue. Treasury is establishing a cyber collaboration center to facilitate greater opportunity for firms to exchange classified and unclassified information and facilitate discussion around threat actor activity and vulnerabilities. Other parts of government have created similar centers such as the NSA's Cybersecurity Collaboration Center. Plans to create a cross-sector equivalent or otherwise foster collaboration and exchange among these efforts would be valuable and CISA could play a helpful role.

Sustaining Progress and Building Capabilities

We are at a defining juncture in CISA's development, similar to any startup at this stage, where achieving scale matters. As Congress intended and supported with funding, CISA must refine its focus and apply resources carefully to be successful. Now that CISA has established its presence, developed communications and outreach capabilities, and designed tools and services to improve near-term resilience, it should shift its approach to expand management capabilities, add operational expertise and establish processes that will be the foundation for sustained leadership on immediate tactical response matters as well as longer-term, proactive planning and support that will benefit even the most cyber-mature sectors like financial services.

Successful implementation of CIRCIA, including harmonizing its reporting requirements to optimize protection and response and streamline coordination, will serve as a cornerstone for the future of public-private partnerships and should be a top priority. Similarly, developing the means to identify and prioritize the highest risks by sector and across sectors will refine CISA's focus and support more secure and resilient outcomes for the nation.

This is no small task and requires CISA to focus on building organizational consistency and rigor, hiring and retaining experienced staff, and sourcing support from sectors that have well-established security, resilience and, in the financial services case, regulatory standards that can be leveraged.

We are committed to working with CISA to support its continued development and look forward to the opportunity to engage in future national risk mitigation efforts.

[6] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. P.L. 116-283, Sec 1715.
[7] National Cybersecurity Strategy, March 2023, p. 15

United States Government Accountability Office

Testimony

Before the Subcommittee on Cybersecurity and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, March 23, 2023

CRITICAL INFRASTRUCTURE PROTECTION

Time Frames to Complete CISA Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities

Statement of Tina Won Sherman, Director, Homeland Security and Justice

GAO-23-106720

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on Sector Risk Management Agencies (SRMAs)—departments or agencies, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise to a sector. My testimony today summarizes the findings from our February 2023 report entitled *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities.*[1] That report examined new responsibilities for SRMAs and the Department of Homeland Security's role in coordinating SRMA activities.[2] [3]

Events have demonstrated how disruption or destruction of the nation's critical infrastructure could have debilitating effects. In particular, the 2021 cyberattack on the Colonial Pipeline disrupted the nation's largest fuel pipeline, and an extreme weather event in Texas caused widespread power and water outages.[4] Such events also illustrate how the nation's critical infrastructure assets and systems are often interconnected with critical infrastructure in other sectors and the internet, making them more vulnerable to attack. Protecting critical infrastructure is a national security priority because it provides essential functions—such as supplying water, generating energy, and producing food—that underpin American society.

The Cybersecurity and Infrastructure Security Agency Act of 2018 assigned the Cybersecurity and Infrastructure Security Agency (CISA) the responsibility to coordinate a national effort to secure and protect against critical infrastructure risks.[5] As such, the Secretary of Homeland

---

[1]GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806 (Washington, D.C.: Feb. 7, 2023).

[2]6 U.S.C. § 665d.

[3]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 outlined these new SRMA responsibilities.

[4]In May 2021, we issued a WatchBlog post addressing the Colonial Pipeline attack and the federal government and private sector response. See https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

[5]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168, 4169 (codified at 6 U.S.C. § 652). The act renamed the Department of Homeland Security's National Protection and Programs Directorate as CISA and outlined CISA's responsibilities.

Security designated the Director of CISA as the national coordinator for critical infrastructure security and resilience. CISA provides a variety of cyber and infrastructure security capabilities and services to federal and non-federal organizations, including assessments and analysis, capacity building, expertise and guidance, and security operations (e.g., incident response).

At the federal level, SRMAs are responsible for leading, facilitating, or supporting the security and resilience programs and associated activities within their designated critical infrastructure sector.[6] The private sector owns and operates the majority of critical infrastructure. Therefore, it is vital that the public and private sectors work together to protect assets and systems.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) includes a provision for GAO to report on the effectiveness of SRMAs in carrying out responsibilities set forth in the act. Our February 2023 report and my statement today addresses (1) how the FY21 NDAA changed sector risk management agency responsibilities, and the actions these agencies reported taking to address them; and (2) the extent to which CISA identified and undertook efforts to help sector risk management agencies implement their responsibilities set forth in the FY21 NDAA.

To address these objectives, we analyzed the FY21 NDAA and relevant policy directives, collected written responses from SRMAs for all 16 sectors using a standardized information collection tool, reviewed other DHS documents, and interviewed CISA officials.[7] Additional information about our scope and methodology can be found in our February 2023 report. Our work was performed in accordance with generally accepted government auditing standards.

[6]6 U.S.C. § 651(5). Presidential Policy Directive-21 (PPD-21) previously called these agencies Sector-Specific Agencies. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 codified Sector-Specific Agencies as SRMAs. In 2013, PPD-21 categorized the nation's critical infrastructure into 16 sectors with at least one federal agency designated as SRMA for the sector, although the number of sectors and SRMA assignments are subject to review and modification. Those designations are still in effect. See 6 U.S.C. § 652a(b). Additionally, some sectors have subsectors, such as the Education subsector within the Government Facilities sector, with the Department of Education having a lead sector risk management role for the subsector.

[7]Three critical infrastructure sectors have co-SRMAs. When co-SRMAs responded to a question with the same answer, we categorized that response as one critical infrastructure sector. In cases where the co-SRMAs for a critical infrastructure sector disagreed, we did not include either of them in the sector count and noted the disagreement.

FY21 NDAA Expanded SRMA Responsibilities, and Agencies Have Actions Underway to Address Them

The FY21 NDAA expanded SRMA responsibilities previously outlined in Presidential Policy Directive-21 (PPD-21) and added risk assessment and emergency preparedness as responsibilities not previously included in the directive for SRMAs.[8] Specifically, prior to the FY21 NDAA, PPD-21 included the following four SRMA responsibilities: (1) serve as a federal interface for the prioritization and coordination of sector-specific activities; (2) carry out incident management responsibilities; (3) provide, support, or facilitate technical assistance and consultations for sectors to support risk management activities; and (4) support the Secretary of Homeland Security by sharing information on sector-specific critical infrastructure. The FY21 NDAA expanded the sector coordination, incident management, risk management, and information sharing responsibilities found in PPD-21 by adding specific activities for SRMAs to carry out within these areas. For example, the FY21 NDAA requires SRMAs to conduct sector coordination activities, including serving as the day-to-day federal interface for the prioritization and coordination of sector-specific activities; serving as federal government coordinating council chair; and participating in cross-sector coordinating councils, as appropriate.

Expanded responsibilities. In response to the expanded responsibilities required by the FY21 NDAA described above, some SRMAs reported having actions underway to address these responsibilities. SRMA officials for four of the 16 critical infrastructure sectors reported adapting activities related to sector coordination, incident management, risk management, or information sharing to address their responsibilities in the act. For example, as SRMA in the healthcare and public health sector, Department of Health and Human Services officials reported coordinating

[8]CISA and the other SRMAs also have roles related to emergency preparedness efforts under the National Preparedness Goal and the National Response Framework. PPD-8 directed the Secretary of Homeland Security to develop a national preparedness goal, which defines the core capabilities necessary for emergency response to specific types of incidents. The National Response Framework is a guide to how the nation responds to disasters and emergencies of all types. The most recent edition of the framework identifies 15 emergency support functions that serve as the federal government's primary coordinating structure for building, sustaining, and delivering response capabilities. According to the framework, existing infrastructure plans and coordination mechanisms such as SRMAs and councils provide strong foundations for strengthening incident response plans and capabilities. As part of the National Infrastructure Protection Plan, the critical infrastructure sectors and SRMAs have developed sector-specific plans. For more information, see Department of Homeland Security, National Response Framework, 4th ed. and GAO, *Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps* [Reissued on December 9, 2015], GAO-15-20 (Washington, D.C.: Dec. 4, 2014).

an effort to analyze the department's existing cyber authorities to identify and mitigate any gaps, as well as developing a cyber-incident response plan.

Additionally, some SRMA officials also reported that activities they established prior to the enactment of the FY21 NDAA already address the responsibilities outlined in the act. For example, SRMA officials from the Department of Energy and the Environmental Protection Agency, representing the energy sector and water and wastewater systems sector respectively, reported that they already address the responsibilities outlined in the FY21 NDAA.

Finally, as an SRMA for eight of the 16 sectors, CISA described established activities that address sector coordination, incident management, risk management, and information sharing. Specifically, CISA officials reported that CISA's Stakeholder Engagement Division focuses on developing relationships with industry and government in CISA's sectors by meeting with Sector Coordinating Councils and issuing advisories and analysis reports to partners.

Added responsibilities. To address the added risk assessment and emergency preparedness responsibilities required by the FY21 NDAA, SRMA officials for five of the 16 critical infrastructure sectors described how they plan to take new actions to address the risk assessment responsibilities outlined in the FY21 NDAA. For example, as SRMA in the communications sectors, DHS officials reported plans to develop and maintain a communications risk register that includes cybersecurity risks to emergency communications infrastructure. SRMA officials for 15 of the 16 critical infrastructure sectors also stated that they had conducted risk assessment activities prior to their inclusion in the FY21 NDAA.[9]

With regard to emergency preparedness responsibilities, SRMA officials for six of the 16 critical infrastructure sectors described how they plan to take new actions to address the emergency preparedness responsibilities outlined in the FY21 NDAA. For example, as SRMA in the financial services sector, Department of the Treasury officials reported enhancing a tabletop exercise program, developing a functional exercise platform to improve cybersecurity exercises, and refining incident management and crisis communication toolkits. SRMA officials for all 16

[9]As the co-SRMAs in the government facilities sector, both DHS Federal Protective Service and General Services Administration officials did not describe conducting prior risk assessment activities. They stated that prior to the FY21 NDAA, non-CISA co-SRMAs were not required to conduct risk assessments for their sector and did not have the authority to require their federal and nonfederal partners to provide responses or submit information for such assessments.

critical infrastructure sectors also stated that they had conducted emergency preparedness activities prior to their inclusion in the FY21 NDAA.

Implementation challenges. SRMA officials cited two challenges in implementing their responsibilities: (1) the voluntary nature of private sector participation in SRMA activities and (2) limited or no dedicated resources for SRMA duties. According to SRMA officials, these challenges pre-dated the enactment of the FY21 NDAA. Additional challenges SRMA officials identified included coordination issues related to inaccurate SRMA point-of-contact lists and government coordinating council and sector coordinating council membership lists, and limited technical cybersecurity expertise. Our past work describing other DHS functions has highlighted the importance of maintaining accurate and up-to-date contact information for the sharing of information.[10]

Participation in SRMA critical infrastructure protection efforts is voluntary, which SRMA officials for 11 critical infrastructure sectors reported as a challenge to conducting their responsibilities. For example, they reported that this affected their ability to stay apprised of issues in the sector and to collect information. SRMA officials reported that these challenges existed prior to the FY21 NDAA and they generally expected them to continue.

SRMA officials also stated that they face challenges because they have limited or no dedicated resources to implement their responsibilities. SRMA officials for 13 of the 16 sectors, including those with and without dedicated resources for SRMA activities, stated that they planned to request additional resources to help them implement their FY21 NDAA responsibilities.

CISA Has Identified and Undertaken Efforts to Help SRMAs, but Does Not Have Milestones and Timelines to Complete Them

CISA has identified and undertaken some efforts that could help SRMAs implement their FY21 NDAA responsibilities. In November 2021, CISA reported on several ongoing and planned efforts to help SRMAs implement these responsibilities and to clarify federal roles and responsibilities for cybersecurity and infrastructure security actions across the federal

[10]See GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017). SRMA officials said they expected CISA to possibly address this challenge if it established consistent communication mechanisms in response to the FY21 NDAA. According to CISA officials, CISA has efforts underway to address issues related to inaccurate points of contact lists.

government.[11] In addition, CISA officials described various efforts to help SRMAs implement their FY21 NDAA responsibilities, including:

Define maturity and effectiveness metrics. CISA officials told us in October 2022 they expect to develop a methodology and metrics to measure the maturity and effectiveness of SRMAs in implementing responsibilities outlined in the FY21 NDAA. For example, in its November 2021 report, CISA recommended that the Federal Senior Leadership Council conduct a sector-by-sector assessment of SRMA partnership participation.[12] CISA officials told us in March 2022 that these efforts could include both standardized metrics to measure effectiveness across all sectors, and sector-specific metrics.

Develop standardized budget guidance. In its November 2021 report, CISA officials identified a need to develop a baseline cost estimation tool for SRMAs.[13] According to the report, this tool would provide SRMAs a baseline estimate of resource needs, and could be tailored to each SRMA. CISA also proposed implementing a consistent resource request process across the SRMAs, which could help address the challenges associated with their resource limitations, as previously discussed. According to CISA officials, this budget formulation tool would allow SRMAs to request sufficient resources to implement their FY21 NDAA responsibilities.

Create sector liaison positions. In August 2022, CISA officials told us they created liaison positions focused on fostering CISA's relationship with SRMAs. According to CISA officials, these liaisons will help CISA respond to the responsibilities outlined in the FY21 NDAA by enhancing communication and coordination with SRMAs, triaging information in response to incidents, and responding to requests for information.

Enhance the Federal Senior Leadership Council. The Federal Senior Leadership Council provides a forum for coordination and communication among agencies with critical infrastructure responsibilities, including SRMAs. The council coordinates implementation of SRMA

[11]In response to the FY21 NDAA, CISA reviewed the framework for securing critical infrastructure and submitted a report to the President and congressional committees that made recommendations. According to CISA officials, they met with and collected feedback from SRMAs while preparing this report. According to CISA officials in January 2023, the President officially approved the recommendations in the 9002(b) report, and initiated the process to rewrite PPD-21. CISA, *FY 2021 National Defense Authorization Act: Section 9002(b) Report*, (Nov. 12, 2021).

[12]CISA, *Section 9002(b) Report*, 42.

[13]CISA, *Section 9002(b) Report*, 5.

responsibilities as well as other initiatives related to protecting critical infrastructure. According to CISA officials, the Federal Senior Leadership Council is intended to be one of the primary ways CISA will coordinate actions to implement the FY21 NDAA across the federal government.

Develop a standardized feedback process. CISA officials told us in June 2022 that they are developing a process to conduct standardized surveys of critical infrastructure stakeholders and plan to use the results to conduct assessments. They said surveys allow them to measure the outcome of sector efforts by collecting information from partners on their intent to take action based on the information, tools, or capabilities provided to them, which they said is important due to the voluntary nature of sector partnerships.

Update the 2013 National Plan and sector-specific plans. CISA officials told us in March 2022 that the updated National Infrastructure Protection Plan (National Plan) will clarify SRMA responsibilities in response to the FY21 NDAA. The National Plan is a key guidance document that provides the overarching national approach for critical infrastructure protection. CISA officials stated that the National Plan will be the "cornerstone" to guide SRMAs as they implement their responsibilities. According to CISA officials, the updated National Plan will: (1) include a revised approach to critical infrastructure protection, (2) provide information on SRMA responsibilities set forth in the FY21 NDAA, (3) clarify federal roles and responsibilities for sector risk management, and (4) outline how government and industry should coordinate to identify and mitigate threats to critical infrastructure. The 2013 update of the National Plan responded to new policy in PPD-21, including an explicit provision that DHS update the National Plan to implement the new directive. CISA officials told us they would not make further updates to the National Plan until the review of PPD-21 is completed.

Further, CISA officials stated in October 2022 they plan to provide additional guidance to SRMAs on how they should update their sector-specific plans. CISA officials told us that the updated sector-specific plans should describe how the sector will implement the updated National Plan, along with efforts tailored to the sector's unique characteristics. CISA officials told us they expected to issue an updated sector-specific plan template 3 to 6 months after the release of the updated National Plan for SRMAs to use in collaboration with their sector partners. Further, they told us that the sector-specific plans would likely take 1 year to develop.

Although CISA has identified and started a number of efforts to help SRMAs implement their FY21 NDAA responsibilities, CISA does not have milestones and timelines to complete its

efforts. According to selected characteristics from GAO's Key Questions to Assess Agency Reform Efforts, government reform efforts should have milestones and timelines to track implementation progress, which can also provide transparency about the progress of reforms.[14]

CISA officials said they had not established milestones and timelines to complete CISA's efforts because the agency has prioritized defining its own role as national coordinator. For example, as of October 2022, CISA officials said they were in the process of developing ways to implement CISA's new authorities under the FY21 NDAA, which requires SRMAs to carry out their responsibilities in coordination with the CISA Director and consistent with DHS strategic guidance.

We recognize that CISA's efforts to address its FY21 NDAA responsibilities are linked to its efforts to mature in its role as national coordinator. However, SRMA officials for all 16 critical infrastructure sectors reported that CISA had not yet provided guidance to help the agencies implement their FY21 NDAA responsibilities. Establishing milestones and timelines, and updating them when necessary, to accomplish its efforts to support SRMAs, would help ensure CISA completes them in a timely manner.

We recommended, and DHS concurred, that the Director of CISA establish milestones and timelines for its efforts to provide guidance and improve coordination and information sharing that would help SRMAs implement their FY21 NDAA responsibilities, and ensure the milestones and timelines are updated through completion.[15] As of March 2023, the agency has not yet implemented the recommendation. CISA officials stated that the Administration's Homeland and Critical Infrastructure Resilience Interagency Policy Committee is in the process of updating PPD-21. Once it is completed, CISA will work to establish the milestones and timelines needed to develop guidance on improving coordination and information sharing.

---

[14]GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts,* GAO-18-427 (Washington, D.C.: June 13, 2018).

[15]GAO-23-105806. GAO has a large body of work examining aspects of critical infrastructure protection and has made over 80 recommendations to SRMAs relevant to the responsibilities outlined in the FY21 NDAA. These recommendations involved sector risk management and assessing sector risk, sector coordination and facilitating the sharing of information regarding physical security and cybersecurity threats, and incident management and contributing to emergency preparedness efforts. As of December 2022, agencies had yet to implement 58 of these recommendations. For more information on these recommendations, see appendix II in GAO-23-105806.

However, as of March 2023, CISA had not developed milestones and timelines to complete its efforts. CISA officials stated that they could not provide a specific timeline for issuing the updated National Plan until the Administration completes a review of PPD-21. CISA officials stated that the Federal Senior Leadership Council has started the Sector Analysis Working Group, which is an interagency consensus-based group that will recommend a new sector designation structure and corresponding SRMA designations. CISA officials reiterated that they plan to issue guidance on improving coordination and information sharing.

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contacts and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Tina Won Sherman, Director, Homeland Security and Justice, at (202) 512-8461 or shermant@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Ben Atwater and Christopher Ferencik (Assistant Directors); Steve Komadina (Analyst-in-Charge); Michele Fejfar; Mike Gilmore; Tracey King; Margaret Ullengren; Haley Wall; and Candice Wright.